合同式をマスターする　by Aokijuku

　合同式を難しいものだと思っている高校生は沢山います。ところが、基礎さえしっかり理解すれば、合同式は決して難しいものではなく、しかも色んな問題に利用出来る極めて便利な道具なのです。これから一緒に合同式を学んで、合同式名人を目指しましょう。

［ 合同式の考え方の基本 ］

　中学生の時に、「５で割って３余る整数と、５で割って４余る整数をかけた数を５で割ったときの余りを求めなさい」といった問題をやったことがありますね。その解答は、きっとこんなふうだったと思います。

　５で割って３余る整数を $5m+3$, ５で割って４余る整数を $5n+4$ （ m , n は整数）とすると

$(5m+3)(5n+4)=25mn+20m+15n+12=5(5mn+4m+3n+2)+2$　　$5mn+4m+3n$ は整数だから

$5(5mn+4m+3n+2)+2$ を5で割ると２余る。

　ところで、この答案の $(5m+3)(5n+4)=25mn+20m+15n+12$ の部分で、実際に求める余りに関係があるのは $3\times4=12=5\times2+2$ 　の部分だけで、他の部分が余りを求めるのに影響を与えることはありません。これを合同式で表すと　$(5m+3)(5n+4)\equiv3\times4\equiv12\equiv2\ (mod5)$ 　となります。ところで、$mod5$ の mod は日本語で「法」と呼ばれ、$mod5$ は5で割ったときの余りを扱っていることを表しています。また、合同式では、≡でつながれた一連の式の最後に $mod5$ のように必ず表記することになっています。

　一般に合同式は２つの数の加法、減法、乗法に利用することが出来、例えば上記の２つの数字 $5m+3$ と $5n+4$ （ m , n は整数）について、加法と減法の場合は以下のようになります。

$(5m+3)+(5n+4)\equiv3+4\equiv7\equiv2\ (mod5)$, $(5m+3)-(5n+4)\equiv3-4\equiv-1\equiv4\ (mod5)$ となります。

（※上の式で減法の場合、$-1=5\times(-1)+4$ 　より、-1を５で割ると商が-1 , 余りが4であることに注意しましょう。）

　これらを中学校でやったやり方で行うと、それぞれ以下のようになります。

　$(5m+3)+(5n+4)=5m+5n+7=5(m+n+1)+2$ 　　$m+n+1$ は整数だから、$5m+3$ と $5n+4$ の和を５で割ると２余る。

　$(5m+3)-(5n+4)=5m-5n-1=5(m-n-1)+4$ 　　$m-n-1$ は整数だから、$5m+3$ と $5n+4$ の差を５で割ると４余る。

　どうですか。合同式って、とても便利でしょう。

［ 合同式の利用 ］

　では、これから合同式を利用して、いくつか問題を解いて見ましょう。

【問題①】 4^{125}を9で割った余りを求めなさい。

　解答　$4^3\equiv64\equiv1\ (mod9)$ 　よって $4^{125}\equiv(4^3)^{41}\times4^2\equiv64^{41}\times16\equiv1^{41}\times16\equiv16\equiv7\ (mod9)$ 　よって求める余りは７

【問題②】 n を11で割ったときの余りが2のとき、n^3+5n+3 を11で割ったときの余りを求めよ。

　解答　$n\equiv2\ (mod11)$ より、$n^3+5n+3\equiv2^3+5\times2+3\equiv21\equiv10\ (mod11)$ 　　よって求める余りは10

【問題③】 　a, b, c は５で割ると余りがそれぞれ１, ２, ３となる自然数とする。$a+2b+3c$ と ab^2c^3 をそれぞれ５で割ったときの余りを求めなさい。　（東洋大学）

　解答　$a\equiv1\ (mod5)$, $b\equiv2\ (mod5)$, $c\equiv3\ (mod5)$ だから、$a+2b+3c\equiv1+2\times2+3\times3\equiv14\equiv4\ (mod5)$

$ab^2c^3 \equiv 1\times 2^2\times 3^3 \equiv 4\times 27 \equiv 4\times 2 \equiv 8 \equiv 3\ (mod5)$　よって、求める余りはそれぞれ4と3となる。

【問題④】 n は自然数とする。次のことを証明せよ。

(1)　$4^{n+2}+5^{2n+1}$　は21の倍数　　(2)　$2^{6n-3}+3^{2n-1}$　は11の倍数

(1) $\boxed{解答}$　$4^{n+2}+5^{2n+1} \equiv 4^n\times 4^2+5^{2n}\times 5 \equiv 4^n\times 16+25^n\times 5 \equiv 4^n\times 16+4^n\times 5 \equiv 4^n\times 21 \equiv 0\ (mod21)$

よって　$4^{n+2}+5^{2n+1}$　は21の倍数であると言える。

(2) $\boxed{解答}$　$2^{6n-3}+3^{2n-1} \equiv 2^{6(n-1)}\times 2^3+3^{2n-2}\times 3 \equiv 64^{n-1}\times 8+9^{n-1}\times 3$

$\equiv 9^{n-1}\times 8+9^{n-1}\times 3 \equiv 9^{n-1}\times 11 \equiv 0\ (mod11)$

よって　$2^{6n-3}+3^{2n-1}$　は11　の倍数であると言える。

【問題⑤】自然数 m を7で割ったときの余りを $\overline{m}$ で表すことにする。

(1)　負でないすべての整数 n に対し，$\overline{5^{n+6}}=\overline{5^n}$ が成立することを証明せよ。

(2)　n が負でない整数のとき，$\overline{5^n}$ の値を求めよ。

(3)　12192^4 を7で割ったときの余りを求めよ。　　(釧路公立大学)

(1) $\boxed{解答}$　$5^6 \equiv (5^2)^3 \equiv 25^3 \equiv 4^3 \equiv 64 \equiv 1\ (mod7)$　よって $5^{n+6} \equiv 5^n\times 5^6 \equiv 5^n\times 1 \equiv 5^n\ (mod7)$　つまり $\overline{5^{n+6}}=\overline{5^n}$ が成り立つ。

(2) $\boxed{解答}$　$\overline{5^{n+6}}=\overline{5^n}$ より、$\overline{5^n}$ は周期が6の周期関数であると言える。よって、$n \equiv 0, 1, 2, 3, 4, 5\ (mod6)$ の6通りについて余りを求めれば良い。

$n \equiv 0\ (mod6)$ のとき　$5^0 \equiv 1\ (mod7)$　　$n \equiv 1\ (mod6)$ のとき　$5^1 \equiv 5\ (mod7)$

$n \equiv 2\ (mod6)$ のとき　$5^2 \equiv 25 \equiv 4\ (mod7)$　　$n \equiv 3\ (mod6)$のとき　$5^3 \equiv 125 \equiv 7\times 19+6 \equiv 6\ (mod7)$

$n \equiv 4\ (mod6)$ のとき　$5^4 \equiv 25^2 \equiv 4^2 \equiv 16 \equiv 2\ (mod7)$　　$n \equiv 5\ (mod6)$ のとき　$5^5 \equiv 5^2\times 5^3 \equiv 4\times 6 \equiv 24 \equiv 3\ (mod7)$

以上より、負でない整数 k について　　$n=6k$のとき $\overline{5^n}=1$、$n=6k+1$ のとき $\overline{5^n}=5$

$n=6k+2$ のとき $\overline{5^n}=4$、　$n=6k+3$ のとき $\overline{5^n}=6$、　$n=6k+4$ のとき $\overline{5^n}=2$

$n=6k+5$ のとき $\overline{5^n}=3$　となる。

(3) $\boxed{解答}$　$12192=7\times 1741+5$　よって　$12192^4 \equiv 5^4 \equiv 2\ (mod7)$　より、求める余りは2となる。